Critical Flaw in Drupal Allow Hackers to Take Control of Websites

18 JULY 19

On Wednesday, Drupal has released a security update addressing a critical vulnerability in the CMS core component allowing hackers to take control of the targeted website.

The vulnerability tracked as CVE-2019-6342 with critical severity rating is an access bypass vulnerability.

According to the advisory, when the experimental Workspaces module is enabled, an access bypass issue is created which can be exploited to take control of the affected websites.

The flaw only affects Drupal 8.7.4 and Drupal 8.7.3 and earlier, Drupal 8.6.x and earlier, and Drupal 7.x are not affected by the issue.

The flaw was discovered by Dave Botsch and reported it to Drupal developers.

Drupal has released version 8.7.5 addressing the issue and all users are advised to update to the new version immediately.

Users who cannot update to version 8.7.5 can patch the flaw by disabling the workspace module.

“For sites with the Workspaces module enabled, update.php needs to run to ensure a required cache clear. If there is a reverse proxy cache or content delivery network (e.g. Varnish, CloudFlare) it is also advisable to clear these as well.”

Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) also released advisory urging users to update their Drupal to version 8.7.5.